



THE UNIVERSITY *of* EDINBURGH

Edinburgh Research Explorer

Quantum magic rectangles: Characterization and application to certified randomness expansion

Citation for published version:

Adamson, SA & Wallden, P 2020, 'Quantum magic rectangles: Characterization and application to certified randomness expansion', *Physical Review Research*, vol. 2, no. 4, 043317.
<https://doi.org/10.1103/PhysRevResearch.2.043317>

Digital Object Identifier (DOI):

[10.1103/PhysRevResearch.2.043317](https://doi.org/10.1103/PhysRevResearch.2.043317)

Link:

[Link to publication record in Edinburgh Research Explorer](#)

Document Version:

Publisher's PDF, also known as Version of record

Published In:

Physical Review Research

General rights

Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.



Quantum magic rectangles: Characterization and application to certified randomness expansion

Sean A. Adamson^{*} and Petros Wallden[†]

School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom



(Received 19 August 2020; accepted 13 November 2020; published 4 December 2020)

We study a generalization of the Mermin–Peres magic square game to arbitrary rectangular dimensions. After exhibiting some general properties, these rectangular games are fully characterized in terms of their optimal win probabilities for quantum strategies. We find that for $m \times n$ rectangular games of dimensions $m, n \geq 3$, there are quantum strategies that win with certainty, while for dimensions $1 \times n$ quantum strategies do not outperform classical strategies. The final case of dimensions $2 \times n$ is richer, and we give upper and lower bounds that both outperform the classical strategies. Finally, we apply our findings to quantum certified randomness expansion to find the noise tolerance and rates for all magic rectangle games. To do this, we use our previous results to obtain the winning probability of games with a distinguished input for which the devices give a deterministic outcome and follow the analysis of C. A. Miller and Y. Shi [SIAM J. Comput. **46**, 1304 (2017)].

DOI: [10.1103/PhysRevResearch.2.043317](https://doi.org/10.1103/PhysRevResearch.2.043317)

I. INTRODUCTION

Quantum theory has been arguably one of the most successful scientific theories, especially in terms of accuracy of predictions and applications. We are currently in the midst of the second “quantum revolution,” where the ability to control quantum systems with great precision has resulted in a new wave of technological applications. What makes quantum theory unique is the fact that our classical intuition frequently fails, and it has been proven that understanding the foundations of this theory is crucial to fully realize the possibilities it offers. Quantum nonlocality and contextuality are two such concepts that conflict with our classical intuition, and at the same time enable one of the most interesting applications: that of device-independent cryptographic protocols. Device-independence, first introduced by Mayers and Yao [1], is the property that allows parties to achieve cryptographic tasks—from key distribution [2] to certified randomness expansion [3], oblivious transfer [4], and secure quantum computation [5]—without trusting the inner workings of their own devices.

Nonlocality is frequently expressed in terms of “guessing” games, in which remote parties that share entanglement try to fulfill a certain winning condition. Finding the optimal winning strategies for quantum and classical parties in these games is the key to using nonlocality for applications such as device-independent cryptography. Mermin [6], Peres [7] introduced one such game called the *magic square game* (see details in Sec. II A). This game has a special place in the

foundations of quantum theory due to two notable properties. Firstly, it is one of the simplest examples where quantum strategies can win with certainty (probability one) while classical strategies cannot. This property is also referred to as *quantum pseudotelepathy* [8] and can be used to illustrate (strong) contextuality in the spirit of the Kochen–Specker Theorem [9]. Secondly, it is the simplest two-player game where the maximal nonlocality can be demonstrated using only Clifford computations [10] (preparation of Bell states and Pauli measurements). In comparison, the CHSH game requires one player to measure in a non-Pauli basis. The magic square game can, in principle, be used for any of the device-independent cryptographic tasks, and its performance in comparison to other games evaluated case-by-case. Furthermore, it can be used for efficient self-testing (e.g., Ref. [11]), another exciting concept made possible by nonlocality. That is, parties can deduce from their purely classical observations the (essentially) exact quantum state they share—a property stronger than simply observing nonclassical correlations.

In this paper, we explore a generalization of the magic square game, the winning probabilities that can be achieved, what qualitative properties are preserved, and how the generalizations can be used in applications. The specific application we focus upon is certified randomness expansion, while analysis of other device-independent cryptographic primitives is deferred to future publications.

Our contributions. We introduce a new class of nonlocal games which we call *magic rectangle* games, characterize their winning probabilities, and apply the results to certified randomness expansion. Note, however, that the term “magic rectangle” has been used differently in the past, to refer to observables arranged into a rectangular array [12,13].

We define a generalization of the Mermin–Peres magic square game to general rectangular dimensions (Definition 1). We fully characterize the optimal winning probabilities for quantum behaviors of all these magic rectangle games (Theorem 13).

^{*}sean.adamson@ed.ac.uk

[†]petros.wallden@ed.ac.uk

In order to achieve this characterization, we first prove a number of general properties, showing that the optimal winning probabilities for any set of behaviors (local, quantum, almost quantum, or nonsignaling) are (i) the same for all games of the same dimension, (ii) symmetric with respect to row/column exchange, and (iii) monotonically increasing with the dimension of the rectangle.

Using the known fact that the regular magic square game (which is a special case of 3×3 magic rectangle games) can be won for quantum strategies with certainty, we reduce the full characterization of magic rectangles to that of $1 \times n$ and $2 \times n$ games (Theorem 2). We also show that the CHSH game, according to our definitions, is a 2×2 magic rectangle game (Theorem 15). We then obtain the optimal winning probabilities for the $1 \times n$ case, while we lower and upper bound the winning probabilities for $2 \times n$ games. To upper bound the probabilities, we conjecture the almost quantum winning probability based on numerical evidence. As a side result, we get that $2 \times n$ games with $n \geq 3$ can be won with certainty using behaviors at level 1 of the NPA hierarchy (and so exhibit a version of “pseudotelepathy”), while the quantum and almost quantum sets both give winning probabilities strictly smaller than unity (thus not exhibiting pseudotelepathy).

Finally, we use this characterization to analyze certified randomness expansion from magic rectangle games. Specifically, we show that the winning probability of an $m \times n$ game with a distinguished input (with deterministic outcomes) can be obtained from the $(m - 1) \times (n - 1)$ game (Theorem 20). This, along with the results of Theorem 13, allows us to determine the noise tolerance (robustness) of each of these games. We then follow the analysis of Miller and Shi [14] to get rates for certified randomness expansion using different magic rectangle games (see Table III).

Related works. The magic square game was introduced by Mermin [6], Peres [7], while Cabello [15,16] and subsequently Aravind [17] stated it as a two-player nonlocal game. Aravind [18] gives a nontechnical demonstration of the Mermin–Peres magic square game. The term quantum *pseudotelepathy* was first introduced by Brassard *et al.* [19], and the magic square game, along with many others that share the property that there exist perfect quantum (but not classical) strategies, were reviewed in Ref. [8]. There are a number of generalizations of the magic square that have been considered in literature. Cleve and Mittal [20] analyze quantum strategies for “binary constraint” games—a general class of games that contains the magic rectangles we define—and give some (weaker than our analysis) upper bounds on winning probabilities from quantum strategies. Arkhipov [21] generalized the magic square and magic pentagram games to be played on hypergraphs called *arrangements*, and characterized which arrangements can exhibit quantum pseudotelepathy. Coladangelo and Stark [22] considered “linear constraint” games, focusing on the uniqueness of winning quantum strategies in order to use such games for self-testing.

To determine optimal quantum strategies, it is important to be able to check if a given experimental behavior admits a quantum model/realization. This question is directly linked with the question of the “degree of nonlocality” present in quantum theory. Navascués *et al.* [23,24] addressed this by giving an infinite hierarchy of conditions that are satisfied by

quantum behaviors, known as the NPA hierarchy. Navascués *et al.* [25] defined the *almost quantum* set of behaviors, which is the set closest to the quantum set that arises in a “natural” way and is easy to check. Sets of behaviors that are easy to handle and include the quantum set, as is the case for the levels of the NPA hierarchy and the almost quantum set, have been used successfully to bound the winning probabilities of quantum parties in many cryptographic settings—something we also exploit in this work.

Certified randomness expansion was first introduced by Colbeck and Kent [3]. Vazirani and Vidick [26] demonstrated quantum security for an exponential expansion protocol. Subsequently, Miller and Shi [27] additionally obtained cryptographic security and robustness. Acín and Masanes [28] reviewed efforts to design device-independent quantum random number generators (up to 2016), and included a comparison of the main protocols. Miller and Shi [14] give the spot-checking protocol that we use for our analysis of certified randomness expansion, and to obtain bounds on expansion rates. Finally, Arnon-Friedman *et al.* [29], Brown *et al.* [30] detail alternative techniques, which give better rates for the spot-checking protocol by using the entropy accumulation theorem [31,32]. These are more involved and case-specific than [14] and, thus, to give a general analysis of certified randomness for all magic rectangle games, we use [14] in our work. Note, however, that the noise tolerance we obtain for the different magic rectangle games does not depend on the specific technique used to bound the rates, and thus applies in general.

Organization of the paper. In Sec. II, we give some background on the magic square game and different levels of correlations. In Sec. III, we define magic rectangle games, and in Sec. IV give some general results for these games. Section V gives a full characterization of the winning probabilities of magic rectangle games. We then apply our results to certified randomness expansion in Sec. VI, and conclude in Sec. VII where we discuss our results and give future directions.

II. PRELIMINARIES

A. The magic square game

The Mermin–Peres magic square game [18] consists of two players, Alice and Bob, who are not allowed to communicate during each round of the game. This could be achieved, for example, by ensuring a spacelike separation between the two players. Each round consists of Alice and Bob respectively being assigned a row and column of an empty 3×3 table uniformly at random, which they must fill according to the rules:

- S1. Each filled cell must belong to the set $\{+1, -1\}$.
- S2. Rows must contain an even number of negative entries (i.e., the product of Alice’s entries to any assigned row must be $+1$).
- S3. Columns must contain an odd number of negative entries (i.e., the product of Bob’s entries to any assigned column must be -1).

Neither player has knowledge of which row or column the other has been assigned, and nor does either player know what

$X \otimes I$	$X \otimes X$	$I \otimes X$
$-X \otimes Z$	$Y \otimes Y$	$-Z \otimes X$
$I \otimes Z$	$Z \otimes Z$	$Z \otimes I$

FIG. 1. A quantum strategy for the magic square game, in which the players share the entangled state $|\Psi\rangle$ given in Eq. (1). Observables X , Y , and Z are the Pauli spin operators, and I is the identity operator. Measurements of Alice correspond to a row, and those of Bob to a column. Each row is formed of mutually commuting observables whose product is equal to I , and each column of mutually commuting observables whose product is $-I$. The eigenvalues of each observable are $+1$ and -1 . These facts combined show rules S1–S3 are automatically satisfied. Moreover, if O_A is any of the given observables for Alice’s system, and O_B is the corresponding observable for Bob’s system, the correlation $\langle \Psi | O_A O_B | \Psi \rangle = 1$ guarantees the players always win.

values the other has entered. The game is won if both players enter the same value into the cell shared by their row and column. It is clear that the optimal classical strategy succeeds with probability $8/9$ only [8], and may be achieved by both players agreeing to each follow a particular configuration for their entire table before the game begins. Strikingly, if the players are allowed to share an entangled quantum state, it is possible for them to win the magic square game with certainty [6,7]. Such games are said to exhibit quantum *pseudotelepathy* [8], setting them apart from many other nonlocal games (including the CHSH game) for which optimal quantum strategies are not guaranteed to win.

A possible quantum winning strategy for the magic square allows the players to share the entangled state

$$|\Psi\rangle = |\Phi^+\rangle_{1,2} \otimes |\Phi^+\rangle_{3,4}, \quad (1)$$

which is the product of two maximally entangled two-qubit Bell states

$$|\Phi^+\rangle_{a,b} \equiv \frac{|0\rangle_a \otimes |0\rangle_b + |1\rangle_a \otimes |1\rangle_b}{\sqrt{2}}. \quad (2)$$

That is, Alice’s quantum system is composed of qubits 1 and 3, and Bob’s system of qubits 2 and 4. Depending on which row and column are assigned, the players make measurements on their respective quantum systems according to the observables given in the corresponding cells of Fig. 1. The outcomes of these determine the values which Alice and Bob should enter into their respective row and column to win with certainty.

Figure 1 shows that, unlike for the CHSH game, optimal quantum strategies for the magic square game can be implemented by performing measurements of the Pauli group only.

B. Levels of correlations

We consider local measurements made on a system shared by two observers, Alice and Bob (multipartite generalizations exist, however, we will only focus on two parties, since it is the setting we consider in this work). Alice chooses an input $x \in \mathcal{X}$ and observes a corresponding measurement output $a \in \mathcal{A}_x$. Similarly, Bob chooses an input $y \in \mathcal{Y}$ and observes a measurement output $b \in \mathcal{B}_y$. We may implicitly assume that inputs for Alice and Bob are distinguishable from one another, and that each output is labeled by its corresponding input. Hence, we may write the sets of all possible outputs for Alice and Bob respectively as the disjoint unions $\mathcal{A} = \bigcup_{x \in \mathcal{X}} \mathcal{A}_x$ and $\mathcal{B} = \bigcup_{y \in \mathcal{Y}} \mathcal{B}_y$. We refer to a fixed configuration of all probabilities $P(a, b | x, y)$ as a *behavior*. These behaviors can also be thought of as vectors in $\mathbb{R}^{|\mathcal{A} \times \mathcal{B}|}$, a convention that is particularly useful for dealing with classes of behaviors that are then mapped to sets of vectors.

Behaviors can be characterized according to properties they have, or according to what physical theories can give rise to such behaviors. The weakest condition (and thus the most general set of behaviors) one typically imposes is that “signaling” should be forbidden; behaviors should not allow for superluminal communication. A behavior is said to exhibit *nonsignaling* correlations [33] if it satisfies both $P(a | x) = P(a | x, y)$ and $P(b | y) = P(b | x, y)$, i.e., the input of one party does not influence the probability of outcomes for the other party. Similarly, a behavior exhibits *quantum* correlations if it is realizable under the laws of quantum mechanics, meaning that there exists a joint state $|\psi\rangle$ and “local” measurement operators $[E_x^a, E_y^b] = 0$ that reproduce the behavior, i.e., such that $P(a, b | x, y) = \langle \psi | E_x^a E_y^b | \psi \rangle$. A behavior exhibits *classical* correlations if there exists a unique joint probability distribution such that the behavior arises as marginals. By a theorem of Fine [34], this also implies that classical behaviors are local. We denote the sets of nonsignaling, quantum, and local behaviors by \mathcal{N} , \mathcal{Q} , and \mathcal{L} , respectively.

Given a behavior, it is not easy to check whether there exists a corresponding quantum model (and thus whether the behavior belongs to \mathcal{Q}). Navascués *et al.* [23,24], in order to characterize the set of quantum behaviors, defined an infinite decreasing hierarchy of nonsignaling correlations (known as the NPA hierarchy). These levels of correlations are intermediate; they are weaker than nonsignaling correlations, but stronger than the quantum set. The different sets of behaviors in the NPA hierarchy are denoted by $\mathcal{Q}_1 \supseteq \mathcal{Q}_2 \supseteq \dots$, and converge to the quantum set in the sense that $\bigcap_{i \geq 1} \mathcal{Q}_i = \mathcal{Q}$. Each set \mathcal{Q}_i can be certified by a different semidefinite program.

A further important set of supraquantum behaviors are the *almost quantum* correlations [25], which we denote $\tilde{\mathcal{Q}} \supsetneq \mathcal{Q}$. It has been argued that this set is special, as it is the smallest set that contains the quantum set and arises naturally from some information theoretic principle (e.g., local orthogonality [35], nontrivial communication complexity [36], etc.). These correlations arise naturally by weakening a single one of the principles defining quantum correlations. Namely, instead of requiring the local measurement operators to commute, one only requires that they commute when acting on the special state that gives the behavior, i.e., $[E_x^a, E_y^b] |\psi\rangle = 0$. It is shown

in Ref. [25] that $\tilde{Q} = Q_{1+AB}$, where Q_{1+AB} is a set of correlations defined in [24] and satisfying $Q_1 \supseteq Q_{1+AB} \supseteq Q_2$ in the NPA hierarchy.

Overall, the above correlations satisfy the inclusions

$$N \supseteq Q_1 \supseteq Q_{1+AB} = \tilde{Q} \supseteq Q_2 \supseteq \dots \supseteq Q \supseteq L. \quad (3)$$

Here, it is worth stressing that the win probabilities in any game can only increase when considering a larger set of behaviors. It follows that to (upper or lower) bound the win probabilities for players of a nonlocal game in one level, one can use other levels of correlations that are easier to deal with. In this work, we will mainly be concerned with the nonsignaling, almost quantum, quantum, and local levels of correlations N , \tilde{Q} , Q , and L respectively, where the almost quantum set is used to upper bound the win probabilities for quantum behaviors.

III. MAGIC RECTANGLE GAMES: DEFINITION

More generally than in Sec. II A, it is possible to construct similar games for arbitrary sizes of magic square; a magic square game with m possible questions for Alice and n for Bob corresponds to an $m \times n$ table. Indeed, this may be more appropriately named a magic *rectangle*. In order to avoid trivially winning classical strategies, we must also generalize the game rules.

Definition 1 (Magic rectangle games). We specify an $m \times n$ game by fixing some $\alpha_1, \dots, \alpha_m$ and β_1, \dots, β_n each belonging to $\{+1, -1\}$, such that their product satisfies

$$\alpha_1 \dots \alpha_m \cdot \beta_1 \dots \beta_n = -1. \quad (4)$$

The rules of the given game are then:

R1. Each filled cell must belong to the set $\{+1, -1\}$.

R2. Upon being assigned the i th row, the product of Alice's entries must be α_i .

R3. Upon being assigned the j th column, the product of Bob's entries must be β_j .

As before, the game is won if both players enter the same value into their shared cell.

Notice that the standard 3×3 magic square game described in Sec. II A is simply the special case where $\alpha_1 = \alpha_2 = \alpha_3 = 1$ and $\beta_1 = \beta_2 = \beta_3 = -1$. In fact, there are 2^{m+n+1} different specifications of $m \times n$ games allowed by Eq. (4).

The requirement of Eq. (4) ensures that no deterministic classical strategy that wins with certainty can exist. In such a strategy, definite values would be assigned to each cell of the table which the players must both follow. The product of all cells would be $\alpha_1 \dots \alpha_m$ when calculated according to the rows, and $\beta_1 \dots \beta_n$ according to the columns, but Eq. (4) is exactly the statement that these products are not equal. Hence, the optimal classical success rate is at most $1 - (mn)^{-1}$. In fact, this success rate is attainable deterministically by Alice and Bob answering according to fixed (but different) tables satisfying rules R1–R3, since such tables can always be constructed which differ in only a single one of their cells (Alice's table need not consider rule R3 and Bob's table need not consider rule R2). We denote this optimal classical success

rate for our $m \times n$ magic rectangle games by

$$\omega_L(m, n) = 1 - \frac{1}{mn}. \quad (5)$$

Let us introduce some further notation to describe our magic rectangle games. We will let X and Y be uniformly distributed random variables taking values in the alphabets $\mathcal{X} = \{1, \dots, m\}$ and $\mathcal{Y} = \{1, \dots, n\}$, respectively, labeling the possible input rows and columns that may be assigned to Alice and Bob. We will denote the possible output rows of Alice and columns of Bob by the random vectors $\mathbf{A} = (A_1, \dots, A_n)$ and $\mathbf{B} = (B_1, \dots, B_m)^T$ with alphabets \mathcal{A} and \mathcal{B} , respectively, where each A_j and B_i takes values in $\{+1, -1\}$. Referring to rules R1–R3, the event that the $m \times n$ magic rectangle game is won upon input $(X, Y) = (x, y)$ is given by

$$W_{x,y}^{m,n} \equiv (A_y = B_x) \cap \left(\prod_{j=1}^n A_j = \alpha_x \right) \cap \left(\prod_{i=1}^m B_i = \beta_y \right). \quad (6)$$

Perhaps more naturally for the games we consider, we can equivalently let \mathcal{A} and \mathcal{B} denote alphabets of the possible question/answer pairs for Alice and Bob allowed by the rules of Definition 1. To illustrate why this is the natural choice, we point out that Alice returning a string of ± 1 's that is not compatible with rule R2 is equally forbidden with her returning the value 5 for one cell, and thus it is the natural choice to exclude such outcomes from the alphabet altogether. This is mathematically expressed as

$$\mathcal{A} = \left\{ (x, \mathbf{a}) \in \mathcal{X} \times \mathcal{A} : \prod_j a_j = \alpha_x \right\}, \quad (7a)$$

$$\mathcal{B} = \left\{ (y, \mathbf{b}) \in \mathcal{Y} \times \mathcal{B} : \prod_i b_i = \beta_y \right\}. \quad (7b)$$

Then, with (X, \mathbf{A}) and (Y, \mathbf{B}) instead taking values in alphabets \mathcal{A} and \mathcal{B} , respectively, the winning event upon input $(X, Y) = (x, y)$ becomes simply

$$A_y = B_x. \quad (8)$$

We will refer to these \mathcal{A} and \mathcal{B} as the *natural* alphabets of a magic rectangle game.

In what follows, we characterize the different sizes of magic rectangle games in terms of their optimal win probabilities and strategies, under different levels of allowed nonsignaling correlations (notably quantum, almost quantum, and general nonsignaling correlations). We will often suppress the numerical values $+1$ and -1 to the symbols $+$ and $-$ for simplicity.

IV. PROPERTIES OF MAGIC RECTANGLE GAMES

To begin our characterization of the magic rectangle games of Definition 1, we first show some general properties of these games, which allow us to narrow the considerations required for a full characterization.

Lemma 5 shows in what sense it is possible to identify games of the same dimension together. Corollary 6 then shows that for magic rectangle games of a given dimension $m \times n$, all choices of specific values for parameters $\alpha_1, \dots, \alpha_m$ and β_1, \dots, β_n satisfying Eq. (4) yield the same optimal win

probability at a given level of allowed correlations Σ . We unambiguously refer to this value as $\omega_\Sigma(m, n)$ and show in Corollary 10 the symmetry $\omega_\Sigma(m, n) = \omega_\Sigma(n, m)$. We show in Corollary 12 that $\omega_\Sigma(m, n)$ is independently increasing in both m and n (with an explicit lower bound given in Lemma 11 in terms of that for smaller magic rectangle games). Finally, the correlation hierarchy of Eq. (3) implies for any particular game

$$\omega_N \geq \omega_1 \geq \omega_{1+AB} \geq \omega_2 \geq \dots \geq \omega_Q \geq \omega_L. \quad (9)$$

Combining these facts leads us to the path we will take towards a characterization, as stated in the following theorem.

Theorem 2. In order to fully characterize quantum (or stronger) optimal strategies for magic rectangle games of arbitrary dimension, it is sufficient to consider only $1 \times n$ games, $2 \times n$ games with $n \geq 2$, and 3×3 games. Moreover, only a single example game for each different dimension need be considered.

Proof. Postponed until the end of this section, after we have shown some general properties of magic rectangle games. ■

Definition 3 (Equivalence of games). We will call two games G and G' *equivalent*, and write $G \sim G'$, if there exist bijections $f: \mathcal{A} \rightarrow \mathcal{A}'$ and $g: \mathcal{B} \rightarrow \mathcal{B}'$ taking the natural alphabets of G to those of G' , such that the winning events are equal. That is, such that $(X', A') = f(X, A)$ and $(Y', B') = g(Y, B)$ imply $W = W'$, where W and W' are the events that each game is won.

Remark. Under Definition 3, given a fixed allowed level for correlations, all equivalent games have the same optimal win probability; strategies are identified with others of equal win probabilities.

Lemma 4. Let $b, b' \in \{0, 1\}^n$ be binary sequences of length $n \geq 2$ with the same parity (that is their Hamming weights are either both odd or both even). Consider the operations $\varphi_{i,j}$ on binary sequences, which have the effect of flipping the bits in both the i th and j th positions. Then, there exists an involutory composition of these operations $\varphi = \varphi_{i_m, j_m} \circ \dots \circ \varphi_{i_1, j_1}$ such that $b' = \varphi(b)$.

Proof. Starting with a binary sequence, we can apply operations $\varphi_{i,j}$ one-by-one in the following way: if there are two or more 1's in the sequence, apply the operation which replaces two of the 1's with 0's. If the initial binary sequence had even parity, repeating this process will eventually yield the sequence of zeros. Else, we will eventually have exactly one nonzero element in position k of the sequence. If it is not already the case, we can apply $\varphi_{1,k}$ to take this to the sequence with exactly one nonzero element occurring in the first position. Hence, we can apply a sequence of these operations, taking each binary sequence to a canonical form depending only on its parity. Since each operation $\varphi_{i,j}$ is involutory, and the operations commute, any sequence of these operations is also involutory and thus invertible. Therefore we may apply some sequence of the operations $\varphi_{i_m, j_m} \circ \dots \circ \varphi_{i_1, j_1}$ taking b to its canonical form, and from its canonical form to b' . ■

Lemma 5. Let G be an $m \times n$ magic rectangle game specified by the parameters $\alpha_1, \dots, \alpha_m$ and β_1, \dots, β_n satisfying Eq. (4), and let G' be a magic rectangle game of identical dimension specified by $\alpha'_1, \dots, \alpha'_m$ and $\beta'_1, \dots, \beta'_n$ also satisfying Eq. (4). Then $G \sim G'$ and, moreover,

there exists an involution F on the set of $m \times n$ games such that $G' = F(G)$.

Proof. Consider the operations $F_{i,j}$ which act on a game with parameters $\alpha_1, \dots, \alpha_m$ and β_1, \dots, β_n to produce an identical game with exception that the sign of both α_i and β_j have been flipped [this is a valid game as Eq. (4) is still satisfied]. Correspondingly, let $f_{i,j}$ and $g_{i,j}$ act on the natural alphabets of the game to produce identical alphabets with the exceptions that each player changes the sign of their output corresponding to the (i, j) th cell of the table. That is, $f_{i,j}(X, A)$ differs from (X, A) in that Alice flips the sign of A_j if her input is $X = i$; similarly, in $g_{i,j}(Y, B)$, Bob flips the sign of B_i if his input is $Y = j$. Upon applying $F_{i,j}$ to a game, the corresponding functions $f_{i,j}$ and $g_{i,j}$ leave the winning event Eq. (8) unchanged for all possible inputs. Moreover, the $f_{i,j}$ and $g_{i,j}$ are bijective when considered as maps to the natural alphabets of the game produced by $F_{i,j}$. Hence, $F_{i,j}$ takes games to equivalent games. We will now show that we can apply some sequence of these operations $F = F_{i_k, j_k} \circ \dots \circ F_{i_1, j_1}$ such that $G' = F(G)$. Transitivity of \sim then shows the desired equivalence.

Consider the parameters of G as a binary sequence $b = (\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$ containing an odd number of negative elements. The operation $F_{i,j}$ applied to G acts to flip the sign of α_i and β_j . Furthermore, we can always construct an operation $F_{i_2, j_2} \circ F_{i_1, j_1}$ which flips the sign of α_{i_1} and α_{i_2} , and similarly an operation $F_{i, j_2} \circ F_{i, j_1}$ which flips the sign of β_{j_1} and β_{j_2} . Thus, by applying a sequence of these operations to G , we can flip the sign of any pair of its parameters in b . Therefore applying Lemma 4 shows the existence of a sequence of these operations $F = F_{i_k, j_k} \circ \dots \circ F_{i_1, j_1}$ such that the game $F(G)$ has parameters given by the binary sequence (also containing an odd number of negative elements) $b' = (\alpha'_1, \dots, \alpha'_m, \beta'_1, \dots, \beta'_n)$. That is, $G' = F(G)$. Finally, since the $F_{i,j}$ are involutory and commute with one another, F is involutory. ■

Corollary 6. Given a fixed correlation level Σ , all magic rectangle games of dimension $m \times n$ have equal optimal win probability, which we denote $\omega_\Sigma(m, n)$.

Proof. G and G' in Lemma 5 are arbitrary $m \times n$ games, and so all games of a fixed dimension are equivalent, and must have equal optimal win probabilities. ■

Definition 7 (Transpose game). We define the *transpose* of an $m \times n$ game G with parameters $\alpha_1, \dots, \alpha_m$ and β_1, \dots, β_n , denoted by G^T , to be the $n \times m$ game specified by the parameters $\alpha_i^T = \beta_i$ and $\beta_j^T = \alpha_j$ for all $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, m\}$.

Lemma 8. Let G be an $m \times n$ magic rectangle game, and fix an allowed level Σ for correlations. If S_Σ is a strategy for G which wins with probability p , then there exists an involution T between strategies, such that the strategy $S_\Sigma^T \equiv T(S_\Sigma)$ for the transpose game G^T also wins with probability p .

Proof. We let T be the map which exchanges the roles of the players in a strategy, so that Bob's former strategy is now played by Alice, and vice versa. In particular, under the action of T , Alice in the transpose strategy S_Σ^T outputs Bob's columns of the strategy S_Σ as rows. Similarly, Bob in S_Σ^T outputs Alice's rows of S_Σ as columns. Such a T is clearly involutory, and preserves the probability assigned to the winning event for magic rectangle games. ■

Lemma 9. Let G be an $m \times n$ magic rectangle game, and let G' be an $n \times m$ magic rectangle game. Fix an allowed level Σ for correlations. If S_Σ is a strategy for G which wins with probability p , then there exists a bijection f between strategies such that the strategy $S'_\Sigma = f(S_\Sigma)$ for G' also wins with probability p .

Proof. Let S_Σ^\top be the transpose strategy of S_Σ , obtained from Lemma 8. Then, S_Σ^\top is a valid strategy for G^\top , which wins with probability p . By Lemma 5, $G' \sim G^\top$, and so there exists a bijection F such that the strategy $S'_\Sigma = F(S_\Sigma^\top)$ for G' also wins with probability p . The required function f is defined by $f(S) = F(S^\top)$. ■

Corollary 10. Optimal win probability is symmetric in the sense that

$$\omega_\Sigma(m, n) = \omega_\Sigma(n, m). \quad (10)$$

Proof. Let S_Σ be an optimal strategy for an $m \times n$ game G , winning with probability p . Suppose that S'_Σ found from Lemma 9 (also winning with probability p) is not optimal for an $n \times m$ game G' . Then, there exists a strategy for G' which wins with probability $q > p$. Again by Lemma 9, this implies the existence of a strategy for G which also wins with probability $q > p$, contradicting the optimality of S_Σ . Hence, S'_Σ is an optimal strategy for G' . Since G and G' were arbitrary, optimal strategies for all $m \times n$ and $n \times m$ games win with equal probability $p = \omega_\Sigma(m, n) = \omega_\Sigma(n, m)$. ■

Lemma 11. Fix a level of allowed correlation Σ . Let the optimal win probability of $m \times n$ magic rectangle games be given by $\omega_\Sigma(m, n)$. If $m' \geq m$ and $n' \geq n$, then the optimal win probability of $m' \times n'$ games satisfies

$$\omega_\Sigma(m', n') \geq 1 - \frac{mn}{m'n'}[1 - \omega_\Sigma(m, n)]. \quad (11)$$

Proof. Let G be an $m \times n$ magic rectangle game specified by the parameters $\alpha_1, \dots, \alpha_m$ and β_1, \dots, β_n . From this, define an $m' \times n'$ game G' such that its parameters are

$$\alpha'_i = \begin{cases} \alpha_i & \text{if } 1 \leq i \leq m, \\ 1 & \text{if } m < i \leq m', \end{cases} \quad (12a)$$

$$\beta'_j = \begin{cases} \beta_j & \text{if } 1 \leq j \leq n, \\ 1 & \text{if } n < j \leq n'. \end{cases} \quad (12b)$$

Note that G' is indeed a valid game, as its parameters automatically satisfy Eq. (4). Let S_Σ be an optimal strategy for G , winning with probability $\omega_\Sigma(m, n)$, in which Alice outputs according to the random row vector $\mathbf{A} = (A_1, \dots, A_n)$ and Bob according to the random column vector $\mathbf{B} = (B_1, \dots, B_m)^\top$. Construct a strategy S'_Σ for G' in which Alice and Bob play their part of the strategy S_Σ upon inputs $1 \leq X' \leq m$ and $1 \leq Y' \leq n$ respectively, but deterministically append 1's to their outputs to make up the required output length; upon other inputs, the players output only 1's. That is,

$$\mathbf{A}' = \begin{cases} (A_1, \dots, A_n, 1, \dots, 1) & \text{if } 1 \leq X' \leq m, \\ (1, \dots, 1) & \text{if } m < X' \leq m', \end{cases} \quad (13a)$$

$$\mathbf{B}' = \begin{cases} (B_1, \dots, B_m, 1, \dots, 1)^\top & \text{if } 1 \leq Y' \leq n, \\ (1, \dots, 1)^\top & \text{if } n < Y' \leq n'. \end{cases} \quad (13b)$$

It is clear that these outputs always satisfy the rules given in Definition 1 for the parameters of G' defined in Eq. (12). Moreover, by using strategy S'_Σ , the players succeed at G' with

probability $\omega_\Sigma(m, n)$ upon mn of the $m'n'$ possible inputs, and with certainty upon the remaining inputs. By Corollary 6, the win probability of S'_Σ at the $m' \times n'$ game G' is at most the optimal win probability for $m' \times n'$ games $\omega_\Sigma(m', n')$. Hence, since the inputs are chosen uniformly at random,

$$\omega_\Sigma(m', n') \geq \frac{mn}{m'n'}\omega_\Sigma(m, n) + \frac{m'n' - mn}{m'n'}, \quad (14)$$

which is exactly Eq. (11). ■

Corollary 12. Fix a correlation level Σ , and let $m' \geq m$ and $n' \geq n$. Then

$$\omega_\Sigma(m', n') \geq \omega_\Sigma(m, n). \quad (15)$$

Proof. Immediate from Eq. (11) upon noting $\frac{mn}{m'n'} \leq 1$ and $\omega_\Sigma(m, n) \leq 1$. ■

Having stated and proven the preceding properties of magic rectangle games, it is now easy to see that Theorem 2 holds as follows.

Proof of Theorem 2. The second part of the claim (that only a single example game for each different dimension need be considered) is shown by Lemma 5 and Corollary 6, which state that all games of the same dimension are equivalent.

For the first part of the claim, we may first choose to consider optimal strategies for $1 \times n$ games. Then, by Lemma 9 and Corollary 10, there are invertible maps between optimal strategies for $n \times 1$ games and $1 \times n$ games. Thus we next study $2 \times n$ games without the need to consider the 2×1 case. Similarly, we then need not consider $n \times 2$ cases. Finally, considering the following observations, we can see that all $m \times n$ games where both $m \geq 3$ and $n \geq 3$ can be won with certainty for quantum (or stronger) behaviors. It was pointed out in Sec. II A that quantum strategies for the standard 3×3 magic square game which win with certainty are already known. As rules S1–S3 for the standard 3×3 magic square game are a special case of our magic rectangle games given in Definition 1, the existence of quantum winning strategies for all general 3×3 games is guaranteed by Lemma 5. Therefore, since by Corollary 12 the quantum value $\omega_Q(m, n)$ is increasing in m and n , and noting the inequalities of Eq. (9), all magic rectangle games with $m \geq 3$ and $n \geq 3$ satisfy $\omega_\Sigma(m, n) = 1$, where Σ is any nonsignaling correlation level at least as strong as the quantum set. Furthermore, the proof of Lemma 11 combined with Lemma 5 shows how to construct winning strategies for all such games from a winning 3×3 strategy. Hence, the 3×3 games already studied are the final case required to complete the characterization of magic rectangle games. ■

V. CHARACTERIZATION OF MAGIC RECTANGLES

Following Theorem 2, we characterize magic rectangle games of all sizes by considering those of dimension $1 \times n$ for $n \geq 1$ and $2 \times n$ for $n \geq 2$. The final 3×3 case was already discussed in Sec. II A.

Theorem 13. The optimal success probabilities of all magic rectangle games can be characterized as follows.

(1) Games of dimension $1 \times n$ cannot exhibit superclassical behavior;

$$\omega_N(1, n) = \omega_L(1, n) = 1 - \frac{1}{n}. \quad (16)$$

(2) Games of dimension $2 \times n$ for $n \geq 2$ satisfy

$$1 - \frac{2 - \sqrt{2}}{2n} \leq \omega_Q(2, n) \leq \omega_{1+AB}(2, n) = \frac{1}{2} \left(1 + \sqrt{1 - \frac{1}{n}} \right), \quad (17)$$

where the final equality is conjectured, with strong numerical evidence for $n \leq 6$. Such games can be won with certainty in the general nonsignaling regime;

$$\omega_N(2, n) = 1. \quad (18)$$

Moreover, for NPA hierarchy level 1 (or stronger) correlations and $n \geq 3$,

$$\omega_1(2, n) = 1. \quad (19)$$

(3) For all quantum or stronger correlations, games of dimension $m \times n$ where both $m \geq 3$ and $n \geq 3$ can be won with certainty;

$$\omega_Q(m, n) = 1. \quad (20)$$

Proof. The content of item 1 is Theorem 14. The discussion in Sec. VB covers item 2. Item 3 was discussed as part of the proof of Theorem 2, and can be seen by combining Corollary 12 with the fact that $\omega_Q(3, 3) = 1$ by Corollary 6. ■

A. 1-by- n magic rectangles

Theorem 14. Under any set of nonsignaling correlations, the optimal win probability of $1 \times n$ games coincides with the classical value,

$$\omega_N(1, n) = \omega_L(1, n) = 1 - \frac{1}{n}. \quad (21)$$

Proof. For all possible inputs $Y = j$ for Bob, his single output value is deterministically equal to β_j according to rule R3 of Definition 1. However, recalling Eq. (4) and denoting the product of Alice's single output row by α , we require any valid $1 \times n$ game to satisfy $\alpha \neq \beta_1 \dots \beta_n$. That is, Alice's output row must contain at least one element, in position k say, which differs from the output value β_k Bob would give if his input was $Y = k$. By the assumption of no-signaling, Alice cannot have any knowledge about which of n possible uniform inputs was provided to Bob. Thus the probability of the losing event that $A_k \neq \beta_k$ (the element of Alice's output corresponding to Bob's input differs from Bob's output) is at least n^{-1} . Therefore $\omega_N(1, n) \leq 1 - n^{-1} = \omega_L(1, n)$. Since trivially also $\omega_N(1, n) \geq \omega_L(1, n)$ by Eq. (9), we have the result. ■

B. 2-by- n magic rectangles

Before discussing the general case of $2 \times n$ magic rectangle games, let us first examine the special case of 2×2 magic square games.

1. 2-by-2 magic squares

In this case, Eq. (4) states that either exactly one of the possible rows or columns is required to have a negative product, or exactly one is required to have a positive product. In fact, any such 2×2 magic square game can be identified with the well-known CHSH game, in which Alice and Bob

are provided binary inputs $X_{\text{CHSH}} \in \{0, 1\}$ and $Y_{\text{CHSH}} \in \{0, 1\}$ uniformly at random, and win by returning binary outputs $A_{\text{CHSH}} \in \{0, 1\}$ and $B_{\text{CHSH}} \in \{0, 1\}$ which satisfy [37]

$$A_{\text{CHSH}} \oplus B_{\text{CHSH}} = X_{\text{CHSH}} \wedge Y_{\text{CHSH}}. \quad (22)$$

We will now explicitly construct this equivalence, whereupon we note the statement $\omega_L(2, 2) = \frac{3}{4}$ defines the unique nontrivial facet of the local polytope in the (2,2,2) Bell scenario (which corresponds also to the CHSH inequality) [34,38].

Theorem 15. Any 2×2 magic square game is equivalent (in the sense of Definition 3) to the CHSH game.

Proof. Consider the 2×2 magic square with specified row products $(\alpha_1, \alpha_2) = (+, +)$ and column products $(\beta_1, \beta_2) = (+, -)$. We first show that this game is equivalent to the CHSH game. Then, since all 2×2 games are equivalent (Lemma 5), the desired result follows by transitivity.

We can identify the input events of the two games as

$$X_{\text{CHSH}} = 0 \longleftrightarrow X = 1, \quad (23a)$$

$$X_{\text{CHSH}} = 1 \longleftrightarrow X = 2 \quad (23b)$$

for Alice, and for Bob

$$Y_{\text{CHSH}} = 0 \longleftrightarrow Y = 1, \quad (24a)$$

$$Y_{\text{CHSH}} = 1 \longleftrightarrow Y = 2. \quad (24b)$$

Alice identifies her two possible outputs as simply

$$A_{\text{CHSH}} = 0 \longleftrightarrow A = (+, +), \quad (25a)$$

$$A_{\text{CHSH}} = 1 \longleftrightarrow A = (-, -). \quad (25b)$$

Bob identifies his outputs depending on his assigned input. If $Y_{\text{CHSH}} = 0$ (equivalently $Y = 1$), then he makes the identifications

$$B_{\text{CHSH}} = 0 \longleftrightarrow B = (+, +)^T, \quad (26a)$$

$$B_{\text{CHSH}} = 1 \longleftrightarrow B = (-, -)^T. \quad (26b)$$

However, if $Y_{\text{CHSH}} = 1$ (equivalently $Y = 2$), then he makes alternative identifications

$$B_{\text{CHSH}} = 0 \longleftrightarrow B = (+, -)^T, \quad (27a)$$

$$B_{\text{CHSH}} = 1 \longleftrightarrow B = (-, +)^T. \quad (27b)$$

These identifications form bijections $f : \mathcal{A}_{\text{CHSH}} \rightarrow \mathcal{A}$ and $g : \mathcal{B}_{\text{CHSH}} \rightarrow \mathcal{B}$ between the natural alphabets of each game, and are explicitly tabulated in Table I.

It remains to show that the winning event for the CHSH game, Eq. (22), and the winning event for the 2×2 magic rectangle game of Eq. (8) upon any input,

$$\bigcup_{x,y \in \{1,2\}} [(A_y = B_x) \cap (X = x) \cap (Y = y)], \quad (28)$$

are identical under the functions f and g . We can rewrite these two events to more closely resemble one another as

$$\bigcup_{x,y \in \{0,1\}} [(A_{\text{CHSH}} \oplus B_{\text{CHSH}} = x \wedge y) \times \cap (X_{\text{CHSH}} = x) \cap (Y_{\text{CHSH}} = y)] \quad (29)$$

TABLE I. The bijections $f: \mathcal{A}_{\text{CHSH}} \rightarrow \mathcal{A}$ and $g: \mathcal{B}_{\text{CHSH}} \rightarrow \mathcal{B}$ used to show the equivalence between the CHSH game and the 2×2 magic square game with parameters $(\alpha_1, \alpha_2) = (+, +)$ and $(\beta_1, \beta_2) = (+, -)$. Elements of the natural alphabets \mathcal{A} , \mathcal{B} , $\mathcal{A}_{\text{CHSH}}$, and $\mathcal{B}_{\text{CHSH}}$ have the form of possible input/output pairs for each game and player, with the input written first.

f		g	
$\mathcal{A}_{\text{CHSH}}$	\mathcal{A}	$\mathcal{B}_{\text{CHSH}}$	\mathcal{B}
(0,0)	(1, (+, +))	(0,0)	(1, (+, +) ^T)
(0,1)	(1, (-, -))	(0,1)	(1, (-, -) ^T)
(1,0)	(2, (+, +))	(1,0)	(2, (+, -) ^T)
(1,1)	(2, (-, -))	(1,1)	(2, (-, +) ^T)

for Eq. (22), and for Eq. (28)

$$\bigcup_{x,y \in \{0,1\}} [(A_{y+1} = B_{x+1}) \cap (X = x + 1) \cap (Y = y + 1)]. \quad (30)$$

One can verify from the identifications made (for example by examining Table I) that terms in the first union above are pairwise equal to those in the second. That is, for all $x, y \in \{0, 1\}$,

$$[(A_{\text{CHSH}} \oplus B_{\text{CHSH}} = x \wedge y) \cap (X_{\text{CHSH}} = x) \cap (Y_{\text{CHSH}} = y)] \\ \equiv [(A_{y+1} = B_{x+1}) \cap (X = x + 1) \cap (Y = y + 1)]. \quad (31)$$

Corollary 16. The maximum probability with which the 2×2 magic square game can be won is (i) $(2 + \sqrt{2})/4 \approx 0.854$ for quantum strategies and (ii) unity for general nonsignaling strategies.

Proof. The result of Theorem 15 means that the maximum attainable win probability for any quantum strategy coincides with that of the CHSH game, namely $(2 + \sqrt{2})/4 \approx 0.854$. For the same reason, under PR box assumptions [39], the 2×2 magic square game can be won with certainty. ■

An example of the identifications made for the 2×2 magic square game considered in the proof of Theorem 15 is depicted in Fig. 2.

2. General 2-by- n games

As stated in Theorem 2, it is enough to consider $n \geq 2$. From Eq. (5), the optimal classical win probability for $2 \times n$ games is given by

$$\omega_L(2, n) = 1 - \frac{1}{2n}. \quad (32)$$

Using the discussion of Sec. VB 1, we can apply Lemma 11 to an optimal 2×2 quantum strategy with value $\omega_Q(2, 2) = (2 + \sqrt{2})/4$ as given by Corollary 16. The win probability of the resulting $2 \times n$ strategy lower bounds the $2 \times n$ quantum value via Eq. (11) as

$$\omega_Q(2, n) \geq 1 - \frac{2 - \sqrt{2}}{2n}. \quad (33)$$

In order to find an upper bound for this quantum value, we have used the implementation of the NPA hierarchy found in the NCPOL2SDPA [40] package with the MOSEK

	—	$\alpha_1 = +$
+	+	$\alpha_2 = +$
$\beta_1 = +$	$\beta_2 = -$	

FIG. 2. Example of the equivalence of the 2×2 magic square and CHSH games. Shown is a filled 2×2 magic square with row products $(\alpha_1, \alpha_2) = (+, +)$ and column products $(\beta_1, \beta_2) = (+, -)$ specified. The input row and column $X = 2$ and $Y = 2$ were chosen for this example. Alice gave output $A = (+, +)$ and Bob gave output $B = (-, +)^T$. The game is won since $A_2 = B_2$. The equivalent input and output configuration for the CHSH game, using the identifications of Table I, are $(X_{\text{CHSH}}, A_{\text{CHSH}}) = (1, 0)$ and $(Y_{\text{CHSH}}, B_{\text{CHSH}}) = (1, 1)$. The CHSH win condition of Eq. (22) is also satisfied.

[41] semidefinite program solver. Optimal values for different $2 \times n$ games and levels of the hierarchy are shown in Table II.

We note that for all levels $1 + AB$ and above that were tested, the optimal value is identical for each $2 \times n$ game, and appears to bound above the quantum value for $n \leq 6$ by the closed-form expression

$$\omega_Q(2, n) \leq \omega_{1+AB}(2, n) = \frac{1}{2} \left(1 + \sqrt{1 - \frac{1}{n}} \right). \quad (34)$$

Furthermore, since the complete bipartite graph $K_{2,n}$ is planar for all n , we know from [[21], Theorem 21] that $\omega_Q(2, n) < 1$. The classical value given by Eq. (32) and the quantum bounds given by Eqs. (33) and (34) are depicted in Fig. 3.

Conjecture 17. The expression for $\omega_{1+AB}(2, n)$ given in Eq. 34 holds for all $n \geq 1$.

Remark. Using the SDPA-GMP [45–47] semidefinite program solver with arbitrary-precision arithmetic, we have been able to verify agreement of Eq. (34) with all but the most computationally intensive entries of Table II to a much higher precision than printed.

Since under general no-signaling assumptions the 2×2 magic square game can be won with certainty (Corollary 16), so too can all $2 \times n$ games with $n \geq 2$ by Corollary 12. It is interesting to note that, as far as the authors are aware, those $2 \times n$ games for $n \geq 3$ examined in Table II are the first examples of nonlocal games with the property that they can be won with certainty using NPA hierarchy level 1 correlations, but only with less than unit probability using almost quantum level $1 + AB$ correlations. An explicit strategy for winning the 2×3 game with certainty using NPA hierarchy level 1 correlations is given in Appendix. Hence, by Corollary 12, the result that $\omega_1(2, n) = 1$ for all $n \geq 3$ is exact.

TABLE II. Optimal win probabilities for $2 \times n$ magic rectangle games, under correlations allowed by different levels of the NPA hierarchy. We see that, for the cases tested, the optimal win probabilities are identical at every level beyond the almost quantum $1 + AB$ level. Moreover, these values appear to follow exactly the expression given in Eq. (34). For $n \geq 3$, we observe games which can be won with certainty at level 1, but with lower than unit probability at the almost quantum and higher levels. Values were obtained through NCPOL2SDPA with the MOSEK solver. Results were also verified with the QETLAB [42] toolbox, using MOSEK [43] within CVX [44].

n	NPA hierarchy level				
	1	$1 + AB$	2	3	4
2	0.8535533906	0.8535533906	0.8535533906	0.8535533906	0.8535533906
3	1.0000000000	0.9082482905	0.9082482905	0.9082482905	0.9082482905
4	1.0000000000	0.9330127019	0.9330127019		
5	1.0000000000	0.9472135955	0.9472135955		
6	1.0000000000	0.9564354646			

VI. APPLICATION TO CERTIFIED RANDOMNESS EXPANSION

In this section, we will be concerned with utilizing the Bell inequality violations provided by magic rectangle games to achieve certified randomness expansion, using the device-independent spot-checking protocol R_{gen} described in [[14], Fig. 2]. The main technical result of this section is to relate the win probabilities of $m \times n$ magic rectangle games with distinguished input, to those of $(m - 1) \times (n - 1)$ games. This enables us to get the optimal noise tolerance of such games, as well as to simply obtain rates for randomness expansion using general magic rectangle games. In terms of rates, there are new techniques that could improve our results, but would need to be examined on a case-by-case basis (see also Sec. VII B).

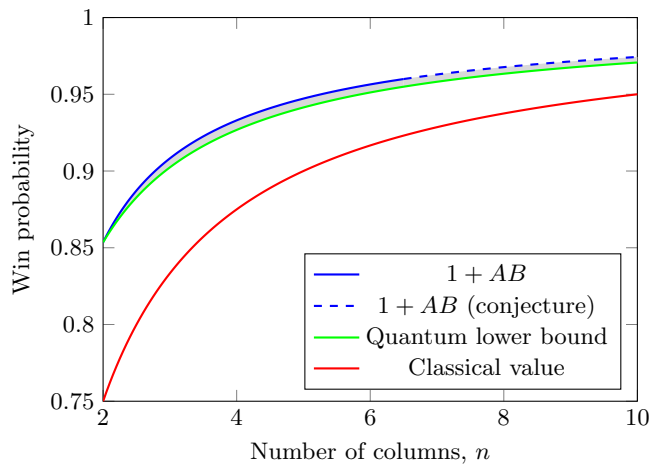


FIG. 3. Bounds on the optimal quantum win probability of $2 \times n$ magic rectangle games. The lowermost curve is the classical value for each game, given by Eq. (32). The middle curve is the lower bound of Eq. (33) on the quantum value of each game, resulting from application of Lemma 11 to the optimal quantum value for 2×2 games. The solid upper curve shows the maximal almost quantum win probability (see NPA hierarchy level $1 + AB$ of Table II), which provides an upper bound to the quantum value; where the line is dashed corresponds to our conjectured values for large n , given by Eq. (34), which have proved to be too computationally intensive to test. The region within which the quantum values could possibly lie is shaded.

Given a nonlocal game, we will denote by ω its optimal win probability over quantum devices, and by $\bar{\omega}$ its optimal win probability over quantum devices with a *distinguished input* (that is, devices which give deterministic outputs upon a single distinguished choice of input). Protocol R_{gen} is shown to produce quantum-secure extractable bits over N rounds, provided its *score acceptance threshold* parameter satisfies $\chi > \bar{\omega}$. In our notation, this result can be stated as

Theorem 18 ([14], Theorem 1.1). For any game, there are functions $\pi : [0, \omega] \rightarrow \mathbb{R}_{\geq 0}$ and $\Delta : (0, 1]^2 \rightarrow \mathbb{R}_{\geq 0}$ such that the following hold:

- (1) For any $b \in (0, 1]$, Protocol R_{gen} produces at least $N[\pi(\chi) - \Delta(b, q)]$ extractable bits with soundness error 3×2^{-bqN} .
- (2) The function π is nonzero on the interval $(\bar{\omega}, \omega]$.
- (3) The function Δ tends to 0 as $(b, q) \rightarrow (0, 0)$.

Modeling noise as a process in which an adversary is allowed to change the outputs of a device arbitrarily with some probability, the noise tolerance of the protocol is $\omega - \chi$ (the adversary is allowed to change the expected score at the game by at most this amount). The noise tolerance is then maximally $\omega - \bar{\omega}$.

Furthermore, an explicit lower bound on the function π was proved in Ref. [14], and can be stated as follows.

Theorem 19 ([14], Theorem 5.8). Let G be a game with output alphabet size $r \geq 2$, and let $\bar{\omega}$ be the maximum win probability of this game over compatible devices with a distinguished input. Then, the following function is a rate curve:

$$\pi(\chi) = \begin{cases} \frac{2(\log_2 e)(\chi - \bar{\omega})^2}{r-1} & \text{if } \chi > \bar{\omega}, \\ 0 & \text{otherwise.} \end{cases} \quad (35)$$

A. Win probability with distinguished input

Since $1 \times n$ magic rectangle games do not exhibit super-classical behavior (Theorem 14), such games cannot be used in randomness expansion. We construct an optimal strategy for arbitrary $m \times n$ magic rectangle games having a distinguished input, where $m, n \geq 2$.

Theorem 20. Fix an allowed level Σ for nonsignaling correlations. The optimal win probability for any $m \times n$ magic rectangle game having a distinguished input, with $m \geq 2$ and

$n \geq 2$, is given by

$$\bar{\omega}_\Sigma(m, n) = 1 - \frac{(m-1)(n-1)}{mn} [1 - \omega_\Sigma(m-1, n-1)]. \quad (36)$$

A strategy which attains this value is to play an optimal strategy for $(m-1) \times (n-1)$ games, but with all output strings extended to include one deterministic entry.

Proof. Without loss of generality, let us choose this distinguished input to be given by the event $(X=1) \cap (Y=1)$. Recall that the event that the game is won upon some input is given in Eq. (6). We will let $W_{x,y} \equiv W_{x,y}^{m,n}$ throughout the following for brevity.

By imposing the no-signaling principle, we see that for all inputs $x \in \{1, \dots, m\}$ and $y \in \{1, \dots, n\}$, there exists an output entry $a^x \in \{+1, -1\}$ for Alice such that

$$\begin{aligned} P(A_1 = a^x | W_{X,Y} \cap X = x \cap Y = y) \\ &= P(A_1 = a^x | W_{X,Y} \cap X = x \cap Y = 1) \\ &= P(B_x = a^x | W_{X,Y} \cap X = x \cap Y = 1) \\ &= P(B_x = a^x | W_{X,Y} \cap X = 1 \cap Y = 1) \\ &= P(B_x = a^x | W_{X,Y} \cap Y = 1) = 1, \end{aligned} \quad (37)$$

where the second equality uses our conditioning on Eq. (6); the first, third, and fourth equalities use no-signaling; and the final equality comes from our choice of distinguished input. Similarly, there exists an output b^y for Bob such that

$$\begin{aligned} P(B_1 = b^y | W_{X,Y} \cap X = x \cap Y = y) \\ &= P(A_y = b^y | W_{X,Y} \cap X = 1) = 1. \end{aligned} \quad (38)$$

Combining Eqs. (37) and (38) yields

$$P(A_1 = a^x \cap B_1 = b^y | W_{X,Y} \cap X = x \cap Y = y) = 1. \quad (39)$$

Now, since for arbitrary events W , E , and F we have

$$P(E | W \cap F) = 1 \Rightarrow P(W | F) = P(W \cap E | F), \quad (40)$$

from Eq. (39) we can see

$$\begin{aligned} P(W_{x,y} | X = x \cap Y = y) \\ &= P(W_{x,y} \cap A_1 = a^x \cap B_1 = b^y | X = x \cap Y = y). \end{aligned} \quad (41)$$

We can now calculate the win probability for a device with a distinguished input. Expanding according to the uniformly distributed input variables and applying the result of Eq. (41) gives

$$\begin{aligned} P(W_{X,Y}) \\ &= \frac{1}{mn} \sum_{x,y} P(W_{x,y} | X = x \cap Y = y) \\ &= \frac{1}{mn} \sum_{x,y} P(W_{x,y} \cap A_1 = a^x \cap B_1 = b^y | X = x \cap Y = y). \end{aligned} \quad (42)$$

It is clear that if $a^1 \neq b^1$ then $W_{1,1} = \emptyset$, and the first term of Eq. (42) vanishes so that $P(W_{X,Y}) \leq 1 - (mn)^{-1}$. Let us now assume that $a^1 = b^1$. In the case where $\prod_{j=1}^n b^j \neq \alpha_1$, we can

bound the terms of Eq. (42), where $X = 1$ as

$$\begin{aligned} \sum_{y=1}^n P(W_{1,y} \cap A_1 = a^1 \cap B_1 = b^y | X = 1 \cap Y = y) \\ \leq \sum_{y=1}^n P(A_y = b^y \cap \prod_{j=1}^n A_j = \alpha_1 | X = 1) \leq n - 1. \end{aligned} \quad (43)$$

Similarly, in the case where $\prod_{i=1}^m a^i \neq \beta_1$, we can bound the terms where $Y = 1$ as

$$\begin{aligned} \sum_{x=1}^m P(W_{x,1} \cap A_1 = a^x \cap B_1 = b^1 | X = x \cap Y = 1) \\ \leq \sum_{x=1}^m P(B_x = a^x \cap \prod_{i=1}^m B_i = \beta_1 | Y = 1) \leq m - 1. \end{aligned} \quad (44)$$

Therefore we have shown $P(W_{X,Y}) \leq 1 - (mn)^{-1} = \omega_L(m, n)$ in all cases other than where

$$(a^1 = b^1) \wedge \left(\prod_{i=1}^m a^i = \beta_1 \right) \wedge \left(\prod_{j=1}^n b^j = \alpha_1 \right). \quad (45)$$

However, in all such remaining cases, combining the above Eq. (45) with the product condition for the α_i and β_j given by Eq. (4), and defining new symbols $\alpha'_i \equiv a^{i+1} \alpha_{i+1}$ and $\beta'_j \equiv b^{j+1} \beta_{j+1}$, yields

$$\alpha'_1 \dots \alpha'_{m-1} \cdot \beta'_1 \dots \beta'_{n-1} = \prod_{i=2}^m a^i \alpha_i \cdot \prod_{j=2}^n b^j \beta_j = -1. \quad (46)$$

We will now assume Eq. (46) to be true in order to completely bound $P(W_{X,Y})$. Further bounding the win probability expansion of Eq. (42) by setting terms conditioned on $X = 1$ or $Y = 1$ to unity, we get

$$\begin{aligned} P(W_{X,Y}) \\ \leq \frac{m+n-1}{mn} + \frac{(m-1)(n-1)}{mn} \\ \times \left[\frac{1}{(m-1)(n-1)} \sum_{y=2}^n \sum_{x=2}^m P(W_{x,y} | X = x \cap Y = y) \right]. \end{aligned} \quad (47)$$

Under a relabeling of the input variables, the square-bracketed terms above coincide exactly with the win probability of an $(m-1) \times (n-1)$ magic rectangle game, with its rules for row and column products specified by $\alpha'_1, \dots, \alpha'_{m-1}$ and $\beta'_1, \dots, \beta'_{n-1}$, respectively. These α'_i and β'_j specify a valid magic rectangle game since they satisfy Eq. (4), as shown by

Eq. (46). Hence, we have the attainable upper bound

$$\frac{1}{(m-1)(n-1)} \sum_{y=2}^n \sum_{x=2}^m P(W_{x,y} | X=x \cap Y=y) \leq \omega_{\Sigma}(m-1, n-1). \quad (48)$$

Combining this with Eq. (47) gives the bound

$$P(W_{X,Y}) \leq \bar{\omega}_{\Sigma}(m, n), \quad (49)$$

where $\bar{\omega}_{\Sigma}(m, n)$ is defined in Eq. (36) as

$$\bar{\omega}_{\Sigma}(m, n) = 1 - \frac{(m-1)(n-1)}{mn} [1 - \omega_{\Sigma}(m-1, n-1)]. \quad (50)$$

We see this has the same form as Eq. (11). Indeed, the proof of Lemma 11 constructs a strategy which attains this bound and is deterministic upon one input. Finally, since

$$\omega_{\Sigma}(m-1, n-1) \geq \omega_L(m-1, n-1) = 1 - \frac{1}{(m-1)(n-1)} \quad (51)$$

for all levels of correlations Σ , Eq. (36) shows the upper bound $\bar{\omega}_{\Sigma}(m, n)$ is always at least that of $1 - (mn)^{-1} = \omega_L(m, n)$ found for the previously considered cases. Therefore $\bar{\omega}_{\Sigma}(m, n)$ represents the complete upper bound on the win probability of an $m \times n$ magic rectangle game with distinguished input and allowed nonsignaling correlation level Σ . ■

B. Performance: Noise tolerance and rates

Lemma 21. The magic rectangle games which can be used in the R_{gen} protocol are those of sizes $2 \times n$ and $3 \times n$ where $n \geq 2$, along with their transposed counterparts.

Proof. We know from Theorem 14 that $1 \times n$ games do not exhibit superclassical behavior, and so cannot be used for randomness expansion. By Theorem 18, then, we seek $m \times n$ games with $m, n \geq 2$ for which $\bar{\omega}_Q(m, n) < \omega_Q(m, n)$. This is clearly not the case for $m, n > 3$, since $\omega_Q(m, n) = 1$ for $m, n \geq 3$, and substituting this into Eq. (36) of Theorem 20 yields $\bar{\omega}_Q(m, n) = 1$ for $m, n > 3$. Thus $\omega_Q(m, n) = \bar{\omega}_Q(m, n)$ for $m, n > 3$. It remains to show that $2 \times n$ games for $n \geq 2$ and $3 \times n$ games for $n \geq 3$ can be used in R_{gen} . Then, the symmetry in $\omega_Q(m, n)$ provided by Lemma 9 (and inherited by $\bar{\omega}_Q(m, n)$ through Eq. (36)) shows that games with transposed dimensions to those may also be used.

Consider the $2 \times n$ games for $n \geq 2$. Using Theorem 14 in Eq. (36) gives

$$\bar{\omega}_Q(2, n) = 1 - \frac{1}{n} < \omega_Q(2, n), \quad (52)$$

where the final inequality is established by comparing with Eq. (33). Now consider the $3 \times n$ games for $n \geq 3$. As in Sec. VB 2, from Ref. [21], we have the upper bound $\omega_Q(2, n-1) < 1$. Again substituting into Eq. (36) of Theorem 20, we get

$$\bar{\omega}_Q(3, n) < 1 = \omega_Q(3, n), \quad (53)$$

where the final equality uses Corollary 12. ■

For the magic rectangle games, which may be used in the protocol R_{gen} (shown in Lemma 21), Theorem 18 results in a

maximum noise tolerance of

$$\rho_{m,n}^{\max} = \omega_Q(m, n) - \bar{\omega}_Q(m, n). \quad (54)$$

Furthermore, combining Theorem 18 with the universal lower bound of Theorem 19 shows that R_{gen} produces (asymptotically in the number of protocol rounds) quantum-secure extractable bits at a rate of at least

$$\pi(\chi) = \frac{2(\log_2 e)(\chi - \bar{\omega})^2}{r - 1} \quad (55)$$

per round, where $\chi \in (\bar{\omega}, \omega]$, and $r \geq 2$ is the total size of the output alphabet for the game. According to rules R2 and R3, a magic rectangle game of dimension $m \times n$ has $2^{m-1} \times 2^{n-1}$ possible outputs. Substituting the result of Theorem 20 for $\bar{\omega}$, this lower bound on the rate can be written for $m \times n$ magic rectangle games as

$$\pi_{m,n}(\chi) = \frac{2(\log_2 e)[\chi - \bar{\omega}_Q(m, n)]^2}{2^{m+n-2} - 1}, \quad (56)$$

where $\bar{\omega}_Q(m, n)$ is as given in Eq. (36). The maximum possible lower bound that Theorem 19 can achieve for the rate then occurs when the score acceptance threshold is set to its maximum $\chi = \omega_Q(m, n)$, such that there is no tolerance to noise, and is given by

$$\pi_{m,n}^{\max} = \pi_{m,n}(\omega_Q(m, n)) = \frac{2(\log_2 e)(\rho_{m,n}^{\max})^2}{2^{m+n-2} - 1}. \quad (57)$$

While this lower bound has the advantage that it only depends only on the dimension of the magic rectangle used, it gives rates that are far from optimal. More practical lower bounds on the rate for the spot-checking protocol could, for example, be calculated based on the techniques of Ref. [29], or numerically as in Ref. [30].

The noise tolerance for the CHSH game, or equivalently the 2×2 magic square game (Theorem 15), is already known to be $(\sqrt{2} - 1)/4 \approx 10.4\%$, and this is confirmed by Eq. (54). Combining our characterization of magic rectangle games from Sec. V with the result of Theorem 20, we summarize the performance of all viable magic rectangle games in Table III. Since the exact quantum values of the 2×2 and 3×3 games are known, inserting Eq. (36) of Theorem 20 into Eq. (54) gives exactly the optimal noise tolerance for R_{gen} using the 3×3 game. Hence, the 3×3 noise tolerance stated in Table III is exact.

It is important to note that, in Table III, the upper bounds given for the noise tolerance and rate of $2 \times n$ games where $n \geq 7$ are calculated based on our Conjecture 17, that Eq. (34) holds for all such n . However, by trivially weakening Eq. (34) to $\omega_Q(2, n) \leq 1$, we can still find less strict upper bounds for these quantities which must hold. Inputting this relaxation into Eqs. (54) and (57), we arrive at

$$\rho_{2,n}^{\max} \leq \frac{1}{2n}, \quad \pi_{2,n}^{\max} \leq \frac{\log_2 e}{2n^2(2^n - 1)}. \quad (58)$$

These expressions are also strictly decreasing with n and, for the conjectural cases of $n \geq 7$, do not exceed the upper bounds for the 2×3 game given in Table III.

TABLE III. All $m \times n$ magic rectangle games which can produce quantum-secure extractable bits in the spot-checking protocol. A selection of specific examples are given in the lower half of the table. Bounds shown for the maximum attainable noise tolerance of $2 \times n$ and $3 \times n$ games are given based on upper and lower bounds for the $2 \times n$ quantum value (see Sec. VB 2). Corresponding bounds are displayed for the maximal universal lower bound on the rate, as given by Eq. (57). For 2×2 and 3×3 games, upper and lower bounds coincide, so their optimal noise tolerance is exact. The $3 \times n$ lower bounds shown for $n \geq 8$ are based on Conjecture 17. The $2 \times n$ upper bounds for $n \geq 7$ are also based on Conjecture 17, but may be more weakly bound as in Eq. (58).

$m \times n$	Noise tolerance $\rho_{m,n}^{\max}$		Rate bound $\pi_{m,n}^{\max}$ (bit/round) ^a	
	Upper bound	Lower bound	Upper bound	Lower bound
2×2	$\frac{1}{4}(\sqrt{2} - 1) \approx 10.4\%$	$\frac{1}{4}(\sqrt{2} - 1) \approx 10.4\%$	≈ 0.01031	≈ 0.01031
3×3	$\frac{1}{9}(2 - \sqrt{2}) \approx 6.5\%$	$\frac{1}{9}(2 - \sqrt{2}) \approx 6.5\%$	≈ 0.00081	≈ 0.00081
$2 \times n$	$\frac{1}{2} \left[\sqrt{1 - \frac{1}{n}} - \left(1 - \frac{1}{n}\right) \right]$	$\frac{1}{2n}(\sqrt{2} - 1)$	$\frac{(\sqrt{n(n-1)} + 1 - n)^2}{2(2^n - 1)n^2 \ln 2}$	$\frac{3 - 2\sqrt{2}}{2(2^n - 1)n^2 \ln 2}$
$3 \times n$	$\frac{1}{3n}(2 - \sqrt{2})$	$\frac{1}{3} \left(1 - \frac{1}{n}\right) \left(1 - \sqrt{1 - \frac{1}{n-1}}\right)$	$\frac{4(3 - 2\sqrt{2})}{9(2^{n+1} - 1)n^2 \ln 2}$	$\frac{2(n-1)(\sqrt{n-2} - \sqrt{n-1})^2}{9(2^{n+1} - 1)n^2 \ln 2}$
2×3	$\frac{1}{6}(\sqrt{6} - 2) \approx 7.5\%$	$\frac{1}{6}(\sqrt{2} - 1) \approx 6.9\%$	≈ 0.00231	≈ 0.00196
2×4	$\frac{1}{8}(2\sqrt{3} - 3) \approx 5.8\%$	$\frac{1}{8}(\sqrt{2} - 1) \approx 5.2\%$	≈ 0.00065	≈ 0.00052
3×4	$\frac{1}{12}(2 - \sqrt{2}) \approx 4.9\%$	$\frac{1}{12}(3 - \sqrt{6}) \approx 4.6\%$	≈ 0.00022	≈ 0.00020
3×5	$\frac{1}{15}(2 - \sqrt{2}) \approx 3.9\%$	$\frac{2}{15}(2 - \sqrt{3}) \approx 3.6\%$	≈ 0.00007	≈ 0.00006

^aThese rates found from Miller and Shi [14] depend only on the dimension of magic rectangle game used. More practical rates could be calculated using the techniques of Refs. [29,30].

VII. DISCUSSION

In this work, we defined a class of nonlocal games which we called “magic rectangles”, since they are natural generalizations of the Mermin [6], Peres [7] magic square. As a first point for future work, it would be interesting to further generalize our games to the multipartite scenario, in which players would output by filling $(d - 1)$ -dimensional slices of a “magic hyperrectangle” of d dimensions. By characterizing a suitable generalization of this kind, it may also be possible to identify other well-known nonlocal games as special cases.

Our main results can be divided into two parts. Firstly, we obtained a full characterization of magic rectangle games with respect to the winning probabilities of quantum and classical strategies. Secondly, we focused on one important application, namely certified randomness expansion; we demonstrated how a complete characterization can be used to explore the potential for device-independent protocols of all the family of nonlocal games we introduced. We will discuss these two parts separately, giving future directions for each.

A. Characterization

We obtained a complete characterization of magic rectangle games. We have shown that $1 \times n$ games cannot exhibit superclassical behavior. Moreover, any magic rectangle game of at least size 3×3 can be won with certainty using quantum or stronger correlations. For these games, the interesting properties of strong contextuality and implementation with only Clifford computations of the regular magic square game are preserved. We have also shown that the special case of dimension 2×2 is identical to the CHSH game, which is well studied and does not exhibit the aforementioned properties.

Finally, the class of $2 \times n$ games for $n \geq 3$ is seen to exhibit the richest behavior: there do not exist perfect quan-

tum winning strategies for these games, however, we have shown superclassical lower bounds on their optimal success probabilities using quantum correlations. We have also given numerical upper bounds on quantum win probabilities for these games with small n , and conjectured a closed-form expression extending to all n . An interesting consequence of our analysis of $2 \times n$ magic rectangle games is that they provide examples of nonlocal games that can be won with certainty using NPA level 1 correlations, and yet for which no quantum (or numerically almost quantum) winning strategy exists (see also Sec. A for an example).

Future works. An interesting future direction is to closer examine this special class of $2 \times n$ magic rectangles. The problem of finding optimal quantum values is still an open question, where the possibilities that they coincide with our lower bounds, upper bounds, or something between all have interesting implications. In the first case, optimal strategies could be implemented using CHSH sub-games. Games of the third case would outperform the CHSH game while also exhibiting a separation between the quantum and almost quantum sets. We believe the second case, in which the quantum and almost quantum sets coincide for each magic rectangle, to be the most likely. This would provide further evidence of the naturality of almost quantum correlations. Once specific strategies (for games beyond CHSH) have been obtained, one could directly see how these perform for various device-independent cryptographic primitives or self-testing.

B. Certified randomness expansion

The optimal noise tolerance of an $m \times n$ magic rectangle game for certified randomness expansion in the spot-checking protocol is fully determined by the difference of the optimal quantum win probability $\omega_Q(m, n)$ and the optimal quantum win probability with distinguished input $\bar{\omega}_Q(m, n)$. In

TABLE IV. The natural alphabets \mathcal{A} and \mathcal{B} defined here denote new notation for the natural alphabets of the 2×3 magic rectangle game under consideration, with parameters $(\alpha_1, \alpha_2) = (+, +)$ and $(\beta_1, \beta_2, \beta_3) = (-, +, +)$. Elements of each alphabet have the form of input/output pairs for each player, with the input written first.

$\mathcal{A}_{2 \times 3}$	\mathcal{A}	$\mathcal{B}_{2 \times 3}$	\mathcal{B}
(1, (+, +, +))	(1,1)	(1, (+, -) ^T)	(1,1)
(1, (+, -, -))	(1,2)	(1, (-, +) ^T)	(1,2)
(1, (-, +, -))	(1,3)	(2, (+, +) ^T)	(2,1)
(1, (-, -, +))	(1,4)	(2, (-, -) ^T)	(2,2)
(2, (+, +, +))	(2,1)	(3, (+, +) ^T)	(3,1)
(2, (+, -, -))	(2,2)	(3, (-, -) ^T)	(3,2)
(2, (-, +, -))	(2,3)		
(2, (-, -, +))	(2,4)		

Theorem 20, we relate $\bar{\omega}_Q(m, n)$ with $\omega_Q(m-1, n-1)$, and given that we have characterized the quantum win probabilities for magic rectangle games of all dimensions in Theorem 13, we can obtain the noise tolerance of all magic rectangle games (Table III). Specifically, the noise tolerance of an $m \times n$ is given as the difference between its quantum value, and the corresponding value of the $(m-1) \times (n-1)$ game extended to dimension $m \times n$ by including in each of its outputs a deterministic entry. It follows that only magic rectangle games of dimension $2 \times n$ and $3 \times n$, with $n \geq 2$ can be used for certified randomness expansion (larger rectangle games fail, since the games can be won with certainty even with a distinguished input). Moreover, we can also see from Table III that the most robust game turns out to be the 2×2 magic square game (which we showed is equivalent to the CHSH game). The values given for general $2 \times n$ and $3 \times n$ games are strictly decreasing with n and, furthermore, of these only the 2×2 and 2×3 games outperform the noise tolerance and rate bound given for the 3×3 game.

From the equivalence with the CHSH game, optimal strategies for the 2×2 game can be implemented using only a single Bell state shared between the players, whereas all known implementations of optimal strategies for the 3×3 game require a system of at least two Bell states. However, implementations of certain winning 3×3 strategies may still be advantageous, for example in cases where physical limitations on the quantum devices dictate certain additional constraints (such as requiring the use of only Clifford gates), or in the context of self-testing (where the use of pairs of Bell states enables parallel self-testing).

Future works. An important remaining question is that of the optimal rates that one can achieve with magic rectangle games. Since we showed that, in terms of noise tolerance, the optimal game coincides with the CHSH game, analysis of the rates has already been done extensively. However, it is still an interesting problem to obtain rates for all the games (whether this is because one is interested in a specific game, or because a protocol may provide better rates with worse noise tolerance—something conceivably possible).

Note that in Table III we do give some rates for all the different games. Theorem 19 directly relates noise tolerance to a lower bound on the rate of randomness expansion, which we can (and do) use to directly obtain indicative rates (Table III last column). However, we would like to stress that the rates obtained from this expression (unlike our noise tolerance analysis) are far from optimal. More practical rates can be calculated, for example, by referring to the techniques outlined in Ref. [29], or numerically as in Ref. [30]. To obtain these improved rates requires an involved, case-by-case analysis that treats each magic rectangle game separately, something that is sensible to do if one is interested in a given game, and is left for future publications.

ACKNOWLEDGMENTS

We would like to thank Matty J. Hoban for useful discussions. S.A.A. gratefully acknowledges EPSRC studentship funding under Grant No. EP/R513209/1.

APPENDIX: WINNING 2-BY-3 GAMES AT NPA LEVEL 1

Consider the 2×3 magic rectangle game in which entries to the first column are required to have a negative product, and all other row and column products are required to be positive. That is, the 2×3 game specified by the parameters $(\beta_1, \beta_2, \beta_3) = (-, +, +)$ and $(\alpha_1, \alpha_2) = (+, +)$ satisfying Definition 1. In order to write our strategy more easily, in Table IV, we introduce a more concise alphabet for the inputs and outputs of the game.

Under the new notation defined in Table IV, the success probability of a behavior $P(a, b \mid x, y)$ where $(x, a) \in \mathcal{A}$ and $(y, b) \in \mathcal{B}$ is

$$\begin{aligned}
 p = \frac{1}{6} & [P(1, 1 \mid 1, 1) + P(2, 1 \mid 1, 1) + P(3, 2 \mid 1, 1) + P(4, 2 \mid 1, 1) \\
 & + P(1, 1 \mid 1, 2) + P(2, 2 \mid 1, 2) + P(3, 1 \mid 1, 2) + P(4, 2 \mid 1, 2) \\
 & + P(1, 1 \mid 1, 3) + P(2, 2 \mid 1, 3) + P(3, 2 \mid 1, 3) + P(4, 1 \mid 1, 3) \\
 & + P(1, 2 \mid 2, 1) + P(2, 2 \mid 2, 1) + P(3, 1 \mid 2, 1) + P(4, 1 \mid 2, 1) \\
 & + P(1, 1 \mid 2, 2) + P(2, 2 \mid 2, 2) + P(3, 1 \mid 2, 2) + P(4, 2 \mid 2, 2) \\
 & + P(1, 1 \mid 2, 3) + P(2, 2 \mid 2, 3) + P(3, 2 \mid 2, 3) + P(4, 1 \mid 2, 3)].
 \end{aligned} \tag{A1}$$

We now state a behavior, achievable using NPA level 1 correlations, for which the win probability p of Eq. (A1) is unity. This behavior is defined via the matrices

$$(P(a, b \mid 1, 1))_{a,b} = \frac{1}{4} \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad (\text{A2a})$$

$$(P(a, b \mid 2, 1))_{a,b} = \frac{1}{4} \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad (\text{A2b})$$

$$(P(a, b \mid 1, 2))_{a,b} = (P(a, b \mid 2, 2))_{a,b} = \frac{1}{4} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (\text{A2c})$$

$$(P(a, b \mid 1, 3))_{a,b} = (P(a, b \mid 2, 3))_{a,b} = \frac{1}{4} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (\text{A2d})$$

Indeed, the behavior defined by Eq. (A2) admits an NPA hierarchy level 1 certificate, given by the matrix

$$\Gamma = \frac{1}{8} \begin{pmatrix} 8 & 2 & 2 & 2 & 2 & 2 & 2 & 4 & 4 & 4 \\ 2 & 2 & 0 & 0 & 1 & -1 & 1 & 2 & 2 & 2 \\ 2 & 0 & 2 & 0 & -1 & 1 & 1 & 2 & 0 & 0 \\ 2 & 0 & 0 & 2 & 1 & 1 & 1 & 0 & 2 & 0 \\ 2 & 1 & -1 & 1 & 2 & 0 & 0 & 0 & 2 & 2 \\ 2 & -1 & 1 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 & 0 & 2 & 2 & 2 & 0 \\ 4 & 2 & 2 & 0 & 0 & 0 & 2 & 4 & 2 & 2 \\ 4 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 4 & 2 \\ 4 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 2 & 4 \end{pmatrix}. \quad (\text{A3})$$

By Corollary 6, we thus have that $\omega_1(2, 3) = 1$. Therefore, by Corollary 12, $\omega_1(2, n) = 1$ for all $n \geq 3$.

-
- [1] D. Mayers and A. Yao, Quantum cryptography with imperfect apparatus, in *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)* (IEEE, 1998) pp. 503–509.
 - [2] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **113**, 140501 (2014).
 - [3] R. Colbeck and A. Kent, Private randomness expansion with untrusted devices, *J. Phys. A Math. Theor.* **44**, 095305 (2011).
 - [4] S. Kundu, J. Sikora, and E. Y.-Z. Tan, A device-independent protocol for XOR oblivious transfer, in *Proceedings of the 15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, edited by S. T. Flammia, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 158 (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2020), pp. 12:1–12:15.
 - [5] A. Gheorghiu, E. Kashefi, and P. Wallden, Robustness and device independence of verifiable blind quantum computing, *New J. Phys.* **17**, 083040 (2015).
 - [6] N. D. Mermin, Simple Unified form for the Major No-Hidden-Variables Theorems, *Phys. Rev. Lett.* **65**, 3373 (1990).
 - [7] A. Peres, Incompatible results of quantum measurements, *Phys. Lett.* **151**, 107 (1990).
 - [8] G. Brassard, A. Broadbent, and A. Tapp, Quantum pseudo-telepathy, *Found. Phys.* **35**, 1877 (2005).
 - [9] S. Kochen and E. P. Specker, *The Problem of Hidden Variables in Quantum Mechanics* (Springer, Dordrecht, 1975), pp. 293–328.
 - [10] D. Gottesman, Theory of fault-tolerant quantum computation, *Phys. Rev. A* **57**, 127 (1998).
 - [11] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, *Quantum* **4**, 337 (2020).
 - [12] C. S. Harvey and J. P. Chryssanthacopoulos, BKS theorem and Bell’s theorem in 16 dimensions, online (2008), visited on 08/10/2020.
 - [13] M. Saniga and M. Planat, Finite geometry behind the Harvey–Chryssanthacopoulos four-qubit magic rectangle, *Quantum Inf. Comput.* **12**, 1011 (2012).
 - [14] C. A. Miller and Y. Shi, Universal security for randomness expansion from the spot-checking protocol, *SIAM J. Comput.* **46**, 1304 (2017).

- [15] A. Cabello, Bell's Theorem without Inequalities and without Probabilities for Two Observers, *Phys. Rev. Lett.* **86**, 1911 (2001).
- [16] A. Cabello, "All Versus Nothing" Inseparability for Two Observers, *Phys. Rev. Lett.* **87**, 010403 (2001).
- [17] P. K. Aravind, Bell's theorem without inequalities and only two distant observers, *Found. Phys. Lett.* **15**, 397 (2002).
- [18] P. K. Aravind, Quantum mysteries revisited again, *Am. J. Phys.* **72**, 1303 (2004).
- [19] G. Brassard, A. Broadbent, and A. Tapp, Multi-party pseudo-telepathy, in *Algorithms and Data Structures* (Springer, Berlin, Heidelberg, 2003), pp. 1–11.
- [20] R. Cleve and R. Mittal, Characterization of binary constraint system games, in *Automata, Languages, and Programming* (Springer, Berlin, Heidelberg, 2014), pp. 320–331.
- [21] A. Arkhipov, Extending and Characterizing Quantum Magic Games, Master's thesis, Massachusetts Institute of Technology (2012).
- [22] A. Coladangelo and J. Stark, Robust self-testing for linear constraint system games (2017), [arXiv:1709.09267](https://arxiv.org/abs/1709.09267) [quant-ph].
- [23] M. Navascués, S. Pironio, and A. Acín, Bounding the Set of Quantum Correlations, *Phys. Rev. Lett.* **98**, 010401 (2007).
- [24] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, *New J. Phys.* **10**, 073013 (2008).
- [25] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín, Almost quantum correlations, *Nat. Commun.* **6**, 6288 (2015).
- [26] U. Vazirani and T. Vidick, Certifiable quantum dice: Or, true random number generation secure against quantum adversaries, in *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing, STOC'12* (Association for Computing Machinery, 2012), pp. 61–76.
- [27] C. A. Miller and Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices, *J. ACM* **63**, 33:1 (2016).
- [28] A. Acín and L. Masanes, Certified randomness in quantum physics, *Nature (London)* **540**, 213 (2016).
- [29] R. Arnon-Friedman, R. Renner, and T. Vidick, Simple and tight device-independent security proofs, *SIAM J. Comput.* **48**, 181 (2019).
- [30] P. J. Brown, S. Ragy, and R. Colbeck, A framework for quantum-secure device-independent randomness expansion, *IEEE Trans. Inf. Theory* **66**, 2964 (2020).
- [31] F. Dupuis, O. Fawzi, and R. Renner, Entropy accumulation, *Commun. Math. Phys.* **379**, 867 (2020).
- [32] F. Dupuis and O. Fawzi, Entropy accumulation with improved second-order term, *IEEE Trans. Inf. Theory* **65**, 7596 (2019).
- [33] L. Masanes, A. Acín, and N. Gisin, General properties of nonsignaling theories, *Phys. Rev. A* **73**, 012112 (2006).
- [34] A. Fine, Hidden Variables, Joint Probability, and the Bell Inequalities, *Phys. Rev. Lett.* **48**, 291 (1982).
- [35] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín, Local orthogonality as a multipartite principle for quantum correlations, *Nat. Commun.* **4**, 2263 (2013).
- [36] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, Limit on Nonlocality in Any World in Which Communication Complexity is not Trivial, *Phys. Rev. Lett.* **96**, 250401 (2006).
- [37] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, *Phys. Rev. Lett.* **23**, 880 (1969).
- [38] S. Pironio, Aspects of quantum non-locality, Ph.D. thesis, Université libre de Bruxelles, 2004.
- [39] S. Popescu and D. Rohrlich, Causality and nonlocality as axioms for quantum mechanics, in *Causality and Locality in Modern Physics* (Springer, Dordrecht, 1998), pp. 383–389.
- [40] P. Wittek, Algorithm 950: Ncpol2sdpa—sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables, *ACM Trans. Math. Software* **41**, 21:1 (2015).
- [41] MOSEK ApS, *MOSEK Optimizer API for Python* (2020), version 9.2.17.
- [42] N. Johnston, QETLAB: A MATLAB toolbox for quantum entanglement (2016), version 0.9.
- [43] MOSEK ApS, *MOSEK Optimization Toolbox for MATLAB* (2020), version 9.2.17.
- [44] CVX Research, Inc., CVX: MATLAB software for disciplined convex programming (2020), version 2.2.
- [45] SDPA Project, SemiDefinite Programming Algorithm, SDPA-GMP (2015), version 7.1.3.
- [46] M. Yamashita, K. Fujisawa, K. Nakata, M. Nakata, M. Fukuda, K. Kobayashi, and K. Goto, *A high-performance software package for semidefinite programs: SDPA 7*, Research Report B-463 (Department of Mathematical and Computing Science, Tokyo Institute of Technology, 2010).
- [47] M. Nakata, A numerical evaluation of highly accurate multiple-precision arithmetic version of semidefinite programming solver: SDPA-GMP, -QD and -DD., in *2010 IEEE International Symposium on Computer-Aided Control System Design* (IEEE, 2010) pp. 29–34.